

1 1. A method of preventing the repudiation of digitally-signed electronic documents,
2 the method comprising the steps of:

3 receiving a plurality of electronic documents during a first and second time
4 interval;

5 forming a message digest for each of the plurality of electronic documents;

6 forming a first super-message digest derived at least in part from each of the
7 message digests received during the first time interval;

8 forming a second super-message digest derived at least in part from each of the
9 message digests received during the second time interval and from the first super-
10 message digest;

11 transmitting the second super-message digest to a timestamp authority and
12 receiving a timestamp therefrom; and

13 recording each of the message digests, first and second super-message digests,
14 and timestamp in an audit log.

1 2. The method of claim 1 wherein at least one of the plurality of electronic
2 documents corresponds to a file attachment in an electronic mail message.

1 3. The method of claim 1 wherein the first and second time intervals are pre-
2 determined.

10 at a web server coupled to the recipient of the encrypted electronic document,
 11 receiving identification data associated with the recipient;
 12 receiving the message parameters transmitted to the recipient;
 13 comparing the identification data associated with the recipient with the received
 14 message parameters;
 15 upon matching the identification data with at least some of the received message
 16 parameters, dynamically computing the symmetric key from the received message
 17 parameters and the hidden parameter associated with the message server using the
 18 predefined algorithm; and
 19 providing the symmetric key to the recipient.

1 9. The method of claim 8 wherein the electronic document is digitally signed.

1 10. The method of claim 8 wherein the message parameters include a recipient list
 2 and a hash of the electronic document.

1 11. The method of claim 8 wherein the electronic document and message parameters
 2 are transmitted to the recipient in an electronic mail message.

1 12. The method of claim 11 wherein the received message parameters are posted to
 2 the web server via an HTML form included in the electronic mail message.

